

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

1/21/2010

SUBJECT:

Multiple Vulnerabilities in Internet Explorer Could Allow Remote Code Execution (MS10-002)

OVERVIEW:

Eight vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of these vulnerabilities. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

One of these vulnerabilities is being actively exploited on the Internet and is referred to as the Aurora exploit.

SYSTEMS AFFECTED:

Microsoft Internet Explorer 6
Microsoft Internet Explorer 7
Microsoft Internet Explorer 8

RISK:

Government:

Large and medium government entities: **High**
Small government entities: **High**

Businesses:

Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:

Eight vulnerabilities have been discovered in Microsoft Internet Explorer. Details of these vulnerabilities are as follows:

Cross Site Scripting Filter Script Handling Vulnerability

An information disclosure vulnerability exists in the way Internet Explorer disables an HTML attribute that correctly filters response data. An attacker could exploit this vulnerability by constructing a specially crafted web page or by posting specially crafted content to a legitimate website. This script code runs inside the browser and requires a user to click on the hypertext link to exploit the vulnerability.

URL Validation Vulnerability

A remote code execution vulnerability exists in the way that Internet Explorer incorrectly validates input. An attacker could exploit this vulnerability by a user clicking on a specially crafted URL. When a user clicks the link, Internet Explorer improperly validates the URL and remote code execution may occur.

Uninitialized Memory Corruption Vulnerabilities

Four remote code execution vulnerabilities exist in the way Internet Explorer accesses an object that has not been correctly initialized or deleted in memory. An attacker can exploit this vulnerability by hosting a specially crafted webpage and a user visits the page. When the user visits the web page, Internet Explorer attempts to access an object that does not exist which can cause the execution of arbitrary code.

HTML Object Memory Corruption Vulnerability

Two remote code execution vulnerabilities exist in the way that Internet Explorer accesses an object that has not been correctly initialized or deleted in memory. An attacker can exploit this vulnerability by hosting a specially crafted webpage and a user visits the page. When the user visits the web page, Internet Explorer attempts to access an object that does not exist which can cause the execution of arbitrary code. **One of these vulnerabilities is associated with the Internet Explorer Zero-Day (Aurora) as first described in Microsoft Security Advisory 979352 and MS-ISAC Advisory 2010-003.**

Successful exploitation of seven of the vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

One of these vulnerabilities is being actively exploited on the Internet and is referred to as the Aurora exploit.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/MS10-002.msp>

<http://www.microsoft.com/technet/security/advisory/979352.msp>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0249>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0248>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0247>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0246>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0245>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0244>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0027>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4074>

VUPEN:

<http://www.vupen.com/english/advisories/2010/0187>

SecurityFocus:

<http://www.securityfocus.com/bid/37883>

<http://www.securityfocus.com/bid/37891>

<http://www.securityfocus.com/bid/37892>

<http://www.securityfocus.com/bid/37815>

<http://www.securityfocus.com/bid/37884>

<http://www.securityfocus.com/bid/37893>

<http://www.securityfocus.com/bid/37894>